AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

FILED
UNITED STATES DISTRICT COURT
ALBUQUERQUE, NEW MEXICO

for the

District of New Mexico

NOV 13 2015 KH

MATTHEW J. DYKMAN
CLERK

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Apple iPhone Model A1532 IMEI 01383800410903

Case No. 15 MR 747

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

located in the _____ District of New Mexico, there is now concealed *(identify the person or describe the property to be seized)*:

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 1028a	Aggravated Identity Theft
18 USC 1546	Fraud, Misuse of Visas, Permits, and other documents

The application is based on these facts:
See affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

_____
Applicant's signature

Ryan Palmiter
Printed name and title

Sworn to before me and signed in my presence.

Date: 11/13/2015

_____
Judge's signature

City and state: Albuquerque, New Mexico

KAREN B. MOLZEN
U.S. MAGISTRATE JUDGE
Printed name and title

In the Matter of the Search of
The property described as:

Apple IPhone, model A1532,
IMEI 013838004109037
Described in Attachment A, incorporated herein by reference

AFFIDAVIT OF SPECIAL AGENT RYAN PALMITER

Your Affiant, Special Agent Ryan Palmiter, from the Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (HSI) being first duly sworn, hereby states as follows:

I. INTRODUCTION

Your Affiant has been employed by Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) since February 18, 2011. Prior to employment with HSI, your Affiant was employed as an Immigration Enforcement Agent, Immigration and Customs Enforcement from March 30, 2008. Your Affiant is currently assigned to the Assistant Special Agent in Charge, Albuquerque, New Mexico office where your Affiant's duties include the investigation of violations of Title 18, United States Code, §1546 and Title 18, United States Code, §1028A.

Your Affiant has successfully completed twelve weeks of Criminal Investigator training at the Federal Law Enforcement Training Center (FLETC). In addition, your Affiant completed nine weeks of Special Agent training with ICE, also at FLETC.

This affidavit is made in support of an application for a search warrant to search the property described as an Apple IPhone, model A1532, International Mobile Equipment Identity (IMEI) 013838004109037, described in Attachment A, and incorporated herein by reference, and to search and seize items.

This affidavit is based upon information your Affiant has gained through training and experience, as well as upon information related to your Affiant by other individuals, including law enforcement officers, whom your Affiant believes to be reliable. Since this affidavit is being submitted for the limited purpose of securing a search warrant, your Affiant has not included each and every fact known concerning this investigation but has set forth only the facts that your

Affiant believes are necessary to establish probable cause to believe that evidence relating to violations of Title 18, United States Code § 1028A and Title 18, United States Code § 1546 are located at the aforementioned property.

Based upon the following information, your affiant submits that there is probable cause to believe that currently located within the above-described property, an Apple IPhone, model A15432, International Mobile Equipment Identity (IMEI) 013838004109037, there is evidence, fruits and instrumentalities of aggravated identity theft, and/or fraud and misuse of visas, permits, and other documents or attempts to do so, in violation of Title 18, United Stated Code §1028A and Title 18, United States Code § 1546, said property more particularly described in Attachment A.

STATUTORY BACKGROUND

This investigation concerns alleged violations of:

Title 18 United States Code, § 1028A, relating to aggravated identity theft.

Title 18, United Stated Code, § 1546, relating to fraud and misuse of visas, permits, and other documents.

CELLULAR PHONES, COMPUTERS AND ELECTRONIC STORAGE

1. As described above and in Attachment B, this application seeks permission to search for and seize records believed to exist on an Apple IPhone, model A15432, International Mobile Equipment Identity (IMEI) 013838004109037, described more particularly in Attachment "A", in whatever form they are found. Upon discovery of records relating to the listed violation, this application seeks permission to include that an Apple IPhone, model A15432, International Mobile Equipment Identity (IMEI) 013838004109037 is identified as a smartphone by its manufacturer. Your Affiant knows from training and experience that smartphones have many of the same capabilities and operating system as a computer and have access to the internet, including web browsers, e-mail programs, and chat programs. One form in which the records might be found is data stored on a computer's hard drive or other storage media to include external storage media connected to the cellular device. Thus, the warrant applied for would authorize the seizure of electronic storage media and the copying of electronically stored information, all under Rule 41(e) (2) (B).
2. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crime described in this warrant,

but also for forensic electronic evidence that establishes how computers or other electronic devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on Apple IPhone, model A15432, International Mobile Equipment Identity (IMEI) 013838004109037, because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of external storage media, and the times the smartphone was in use. Smartphone file systems can record information about the dates files created and the sequence in which they were created.

b. Forensic evidence on a smartphone or storage medium can also indicate who has used or controlled the smartphone or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the smartphone or storage medium at a relevant time.

c. A person with appropriate familiarity with how a smartphone works can, after examining this forensic evidence in its proper context, draw conclusions about how the smartphone was used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium, such as a smartphone, that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the smartphone and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer or other electronic device, such as a smartphone, was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) along with passwords, encryption keys and other access devices, may be relevant to establishing the user's intent.

3. In most cases, a thorough search of Apple IPhone, model A15432, International Mobile Equipment Identity (IMEI) 013838004109037, for information stored on storage media requires the seizure of the physical storage media and later off-site review consistent with the warrant. Seizure is necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

   a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer or smartphone has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

   b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

   c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats and may require off-site reviewing with specialized forensic tools. Formats may include flash memory cards in various formats with the associated storage capabilities of the cellular device.

4. Your affiant also knows that electronic storage devices (like smartphones) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order and with deceptive

file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data store, and it would be generally impossible, due to the equipment needed and the time necessary to accomplish this kind of data search on-site.

5. Your affiant is additionally aware that searching smartphones for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. Since cellular phone evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.
6. Based on your affiant's knowledge, training, and experience, your affiant knows that smartphone storage files or remnants of such files can be recovered months or even years after they have been downloaded onto the internal memory, deleted or viewed via the Internet. Even when files have been deleted, they can be recovered months or years later using forensics tools. This is so because when a person "deletes" a file on a cellular phone, the data contained in the file does not actually disappear; rather, that data remains on the internal memory until it is overwritten by new data.
7. Based on your affiant's knowledge, training, and experience, your affiant knows that smartphone are often used by those involved in identity theft and misuse of identity documents whether that be communicating with coconspirators, the document maker, receiving or sending photos to be used for the document, or sending examples or the finished document to buyers.

DETAILS OF INVESTIGATION

1. On October 15, 2015, Homeland Security Investigations (HSI) Albuquerque, New Mexico arrested Noe PIMENTEL. PIMENTEL was detained by the Albuquerque Aviation Police Department after the Department of Homeland Security Transportation Security Administration (TSA) conducted a baggage screen and subsequent search of PIMENTEL's checked bag

2. TSA's search of PIMENTEL's bag revealed eight (8) fraudulent United States Passport Cards, five (5) fraudulent New Mexico Driver Licenses in PIMENTEL's likeness, three (3) fraudulent Ohio Driver Licenses, and numerous new mobile phones.

3. Your Affiant made contact with a victim identified in this investigation referred to hereinafter as LT. LT's name and address were on one of the New Mexico Driver Licenses in PIMENTEL's likeness. LT stated four (4) mobile phones were charged to his

mobile provider account. These phones were picked up at a Best Buy store in Tucson, Arizona. LT did not authorize this transaction.

4. Thirteen (13) Best Buy electronic gift card receipts were found in PIMENTEL's bag.

5. Travel receipts show PIMENTEL was traveling with two (2) other coconspirators from New York to New Mexico with travel to Arizona and Texas.

6. PIMENTEL was in possession of three (3) mobile phones at the time of his arrest.

CONCLUSION

1. Based upon the information contained in this affidavit, your Affiant has reason to believe that records, evidence, fruits and instrumentalities relating to violations of Title 18, United Stated Code § 1028A and Title 18, United States Code § 1546, exist in the above described property.

2. WHEREFORE, your Affiant respectfully requests that a warrant be issued authorizing the agents of Homeland Security Investigations, with appropriate assistance from other law enforcement officers, to search for, seize, and analyze Apple IPhone, model A15432, International Mobile Equipment Identity (IMEI) 013838004109037, for items set forth in Attachment A, incorporated herein by reference, for said evidence, fruits and instrumentalities related violations of Title 18, United States Code § 1028A – Aggravated Identity Theft, and Title 18, United States Code § 1546 –Fraud and Misuse of Visa, Permits, and other documents.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Ryan Palmiter, Special Agent
Homeland Security Investigations

Sworn to and subscribed before me this 13th day of November 2015, in Albuquerque, New Mexico

United States Magistrate Judge

ATTACHMENT A
DESCRIPTION OF PROPERTY TO BE SEARCHED

The PROPERTY described as a white in color Apple IPhone, model A15432, International Mobile Equipment Identity (IMEI) 013838004109037, currently in the possession of Homeland Security Investigations at 5441 Watson Drive SE Albuquerque, NM 87106.

KBM

ATTACHMENT B

DESCRIPTION OF PROPERTY TO BE SEARCHED FOR AND SEIZED

Items to be searched, seized and analyzed include all evidence, fruits and instrumentalities pertaining to violations of Title 18, United States Code § 1028A – Aggravated Identity Theft and Title 18, United States Code § 1546 – Fraud and Misuse of Visas, Permits, and other documents, and contained within the cellular phone Apple IPhone, model A15432, International Mobile Equipment Identity (IMEI) 013838004109037, any contact lists, call histories, text messages, photographs, videos, Internet history, and other evidence of related transactions to identity theft and/or fraud/misuse of visas permits and other documents;

1. Records and electronically stored message documents that show the communications concerning identity theft and/or fraud/misuse of visas permits and other documents;
2. Smartphone, smartphone hard drives, or other physical objects upon which computer data can be recorded that is called for by this warrant, or that might contain things otherwise called for by this warrant including:
   a. Evidence of who used, owned, or controlled the Apple IPhone, model A15432, International Mobile Equipment Identity (IMEI) 013838004109037 at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence.
   b. Evidence of software that would allow others to control Apple IPhone, model A15432, International Mobile Equipment Identity (IMEI) 013838004109037, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.
   c. Evidence of the lack of such malicious software;
   d. Evidence of the attachment to the Apple IPhone, model A15432, International Mobile Equipment Identity (IMEI) 013838004109037 of other storage devices or similar containers for electronic evidence.
   e. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Apple IPhone, model A15432, International Mobile Equipment Identity (IMEI) 013838004109037.
   f. Evidence of the times the Apple IPhone, model A15432, International Mobile Equipment Identity (IMEI) 013838004109037 was used.
   g. Passwords, encryption keys, and other access devices that may be necessary to access the Apple IPhone, model A15432. International Mobile Equipment Identity (IMEI) 013838004109037.
   h. Contextual information necessary to understand the evidence described in this attachment.

KBM

i. Records of internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.

3. During the course of the search, photographs of the searched property may also be taken to record the condition thereof and/or the location of items therein.